

Mr Timothy Pilgrim  
Privacy Commissioner  
Office of the Australian Information Commissioner  
GPO Box 5218  
SYDNEY NSW 2001  
Email: [consultation@oaic.gov.au](mailto:consultation@oaic.gov.au)

12 April 2013

**Consultation – Guidelines for developing codes  
issued under Part IIIB of the *Privacy Act 1988***

Dear Mr Pilgrim

Thank you for the opportunity to comment on the Office of the Australian Information Commissioner's *Guidelines for developing codes issued under Part IIIB of the Privacy Act 1988*.

The Australasian Retail Credit Association (ARCA) is the industry association for retail Credit Providers and Credit Reporting Bodies as defined in the *Privacy Act (Cth) 1988* (the Privacy Act). ARCA exists to promote best practice in credit risk assessment and responsible credit, as well as to promote better standards in consumer credit reporting. ARCA takes a leadership role in promoting the sharing of information to enable Credit Providers to better serve their customers.

ARCA notes that our comments are made in the context of you appointing ARCA as the developer of the Credit Reporting Code of Conduct (CR Code), in accordance with s 26P in Schedule 3 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (the Privacy Amendment Act).

The draft CR Code is open for public comment on ARCA's website (<http://www.arca.asn.au/CRCodeConsultation>) until 5 May 2013. In accordance with our appointment by you, we intend to submit the CR Code to you for registration by 1 July 2013.

ARCA notes that at its core the credit reporting legislative framework in Australia is a unique combination of

- the Privacy Act,
- supporting regulations (which have yet to be completed), and
- a code of conduct approved and registered by the OAIC which will be binding on all credit providers and credit reporting bodies (as defined by the Privacy Act) that will mandatory, and operate as a legislative

instrument whereby a contravention of the CR Code will be a contravention of the Act.

Further, ARCA Members – who account for a reported 80% or more of data in the credit reporting system – believe that these fundamental reforms will require the introduction of additional business to business elements to the credit reporting system including a data standard to govern exchange between credit providers and credit reporting bodies, categorisation of data exchanged into tiers, and an externally monitored system of data exchange reciprocity between credit providers and credit reporting bodies.

ARCA is in the process of developing the industry framework associated with the additional elements that will cover the activities of our Members and other organisations that agree to be bound by the framework.

### **One single guideline**

Whilst ARCA fully supports the release of OAIC guidance with respect to the drafting of privacy codes, we have a fundamental concern that the mixing of guidance on the CR Code with other codes has the potential to cause confusion.

Whilst ARCA recognises that the CR Code will have many of the same characteristics of privacy codes, and thus much of the guidance for both types of codes will be similar, the CR Code is nonetheless a fundamentally different type of document. The CR Code is a legal instrument, will hold its own Division in the Privacy Act, is required by s 26S(4) of the Act, and – as with other registered codes – a contravention of the CR Code is a contravention of the Act.

Consequently, ARCA recommends that a separate guideline is released by the OAIC to specifically cover the CR Code.

### **Role of code administrator in the CR Code**

In sections 2.26 to 2.28, the guideline indicates that the OAIC expects code developers to have in place, as part of the ongoing code governance, mechanisms for the regular monitoring and reporting by code administrators to the Commissioner of information regarding the code's effectiveness in achieving compliance from entities bound by the code. These mechanisms should include auditing for, or investigating, serious or repeated interferences with privacy or systemic issues related to compliance with a code.

The Privacy Amendment Act does not state that the CR Code will be an industry-owned code, despite you appointing an industry body to draft it on your behalf. The strong belief of ARCA Members is that the role of the code

administrator with respect to the CR Code should be limited to developing the Code, and conducting periodic reviews and recommending changes to the CR Code. Members consider that this role should not include activities such as audits and investigations that are more appropriately within the province of the regulator designated by the legislation to oversee and enforce the Code.

ARCA Members are concerned with the additional costs associated with another layer of monitoring and compliance associated with the credit reporting system, particularly with respect to the requirements of s. 20N of the Privacy Amendment Act.

ARCA Members believe that the roles played by CRBs, external dispute resolution schemes and the OAIC in credit reporting make the appointment of a code administrator unnecessary.

The draft guideline, at 2.27, notes four specific activities that code administrators are expected to undertake. ARCA will address each of these activities in turn, namely:

*"...provide, by 31 July each year, a report to the Commissioner covering the 12 month period ending on 30 June of the same year, to enable the Commissioner to include information about registered codes in the Office of the Australian Information Commissioner (OAIC)'s annual report. However, serious or repeated interferences with privacy in relation to compliance with the Code should be reported as soon as the code administrator becomes aware of them...."*

ARCA notes that the foundation of such a report to the OAIC on the operation of the CR Code would be the annual audits by CRBs of credit providers as required by the Privacy Amendment Act at s 20N and 20Q. At present the CR Code is constructed whereby these audits would be reported to the OAIC, not to an alternative organization – the code administrator.

*"...provide accurate, up to date and sufficient information in the report, including in relation to any systemic issues, or serious or repeated interferences with privacy that have occurred during the year, for the Commissioner, stakeholders and the general public to make a fully informed judgment on the code's effectiveness in achieving compliance from entities bound by the code. In relation to codes which have internal privacy complaint handling procedures, if there are any privacy complaints made by individuals to the entities bound by the code about non-compliance with the code, this will need to be included in the report (see Part 5)"*

The audits which the CRBs will undertake to satisfy s 20N(3)(b) of the Privacy Amendment Act could form the basis for the code administrator's monitoring

activities which could then be managed to meet the requirements of the OAIC outlined above. However, ARCA notes that at present the CR Code draft contemplates that CRBs will be able to meet their audit obligations by conducting audits through a risk-based assessment of requirements, perhaps in partnership with an annual self-attestation of compliance. As the CR Code is likely to meet the 'internal privacy complaint handling procedures' trigger in the draft guideline, these would only be able to be reported in accordance with the risk-based methodology as anticipated.

*"...where information regarding a code's effectiveness in achieving compliance has significantly changed from the last report, provide a description of the change and the reasons for the change."*

ARCA notes with respect to this commentary that it should be clear that the CR Code, as a legal instrument, will likely contain specific clauses regarding amending the document. Therefore, the commentary requested in the guide would be limited to changes in process and industry practice – not the CR Code itself.

*"...publish the report online."*

ARCA notes that the proposal that the report containing specific information pertaining to breaches to be published online is a harsh requirement, and is likely to lead to significant concern by industry participants.

### **Head of power & practicality of code administrator role for CR Code**

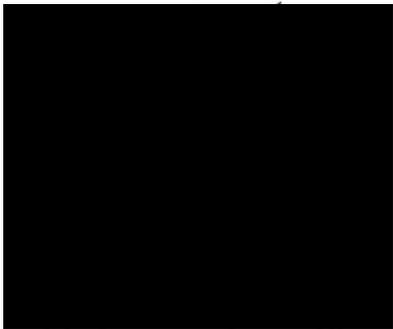
ARCA notes that the role of a code administrator for the CR Code was not envisaged by industry prior to the release of the OAIC draft guideline, was not a feature of the previous credit reporting environment, and was not raised in any public forum we attended prior to the release of the draft guideline. Further, there are significant practical problems with the proposal to require a code administrator with respect to the CR Code.

For example, the audits which the CRBs will undertake to satisfy s 20N(3)(b) of the Privacy Amendment Act could form the basis for the code administrator's monitoring activities. However, it is not clear to ARCA where the head of power for the code administrator to receive those audits would come from. ARCA notes also the expectation that the code administrator would be properly resourced – but in the context of a compulsory code where there are no 'subscribers' as such, again how a levy or some other mechanism could be applied across thousands of organisations by a private entity is not clear.

Finally, the expectation that a register of organisations covered by the code is maintained again seems to lend itself to an APP code where organisations choose to subscribe. In the case of the CR Code, where many thousands of organisations will be covered by the operation of the code by virtue of business activities and without subscribing, establishing and then maintaining such a register would be extremely difficult. Further, at 2.17 the draft guideline suggests that every relevant organisation's trading and legal names are to be included in the register. In case of some ARCA Members they would have more than a dozen legal and trading names each – increasing exponentially the size of the register.

For any additional information or comment regarding this submission, please contact [REDACTED], ARCA Head of Public Affairs, on [REDACTED] or email [REDACTED]

Yours sincerely



**Chief Executive Officer**